

STEVEN G. KALAR
Federal Public Defender
GABRIELA BISCHOF
Assistant Federal Public Defender
450 Golden Gate Avenue
San Francisco, CA 94102
Telephone: 415.436.7700
Facsimile: 415.436.7706
Gabriela_Bischof@fd.org

Counsel for Defendant COFIELD

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,

Plaintiff,

v.

RAMON COFIELD,

Defendants.

Case No. CR 19-00100-VC

**DEFENDANT'S MOTION TO
SUPPRESS AND REQUEST FOR
EVIDENTIARY HEARING**

TO: THE UNITED STATES OF AMERICA, PLAINTIFF; DAVID ANDERSON, UNITED STATES ATTORNEY; AND ANKUR SHINGAL, ASSISTANT UNITED STATES ATTORNEY

PLEASE TAKE NOTICE that on January 19, 2021, at 10:30 a.m., or as soon thereafter as the matter may be heard, in the courtroom of the Honorable Vince Chhabria, counsel for defendant Ramon Cofield will move this Court for entry of an order requiring the government to produce documents related to its investigation in this case. This motion is based on the Fourth Amendment's warrant requirement, all relevant case law and statutory authority, the following memorandum of points and

authorities, any reply memorandum, and any oral argument made at the motion hearing. Should any disputed issue of material fact arise with respect to this motion to suppress, Mr. Cofield further moves this Court for an evidentiary hearing.¹

//

//

\\

//

¹ Mr. Cofield respectfully requests the right to make additional motions to suppress as appropriate based on the Court's rulings, and also to seek to exclude any evidence at trial under Fed. R. Evid. 403 and 404(b).
U.S. v. Cofield, Case No. CR 19-00100-VC
DEF'S MOTION TO SUPPRESS

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iv
INTRODUCTION	1
FACTUAL BACKGROUND.....	1
I. Tumblr’s CyberTip and the NCMEC Report.....	2
II. The Search Warrants	3
III. Google Products	5
IV. Tumblr and Law Enforcement.....	7
V. NCMEC	9
ARGUMENT.....	10
I. The Government Bears the Burden of Proving That the Warrantless Searches Fell Within an Exception to the Fourth Amendment’s Warrant Requirement	10
II. SFPD’s State Search Warrants Were Invalid.....	14
A. The Probable Cause Statements Relied Primarily Upon the Fruits of Tumblr, NCMEC, and SFPD’s Presumptively Unconstitutional Searches	14
B. Sergeant Castillo Made False Statements and Omitted Critical Information In Her Warrant Applications	15
C. The State Search Warrant Failed to Meet the Fourth Amendment’s Specificity Requirement..	25
D. The Tumblr and Google Search Warrants Lacked Probable Cause	27
III. The Warrants Issued to Search AT&T and Mr. Cofield and His Residence Were Invalid....	29
CONCLUSION	29

TABLE OF AUTHORITIES

Federal Cases

<i>Chism v. Washington</i> , 661 F.3d 380 (9th Cir. 2011)	22
<i>Franks v. Delaware</i> , 438 U.S. 154 (1978)	15, 21, 24
<i>George v. Edholm</i> , 752 F.3d 1206 (9th Cir. 2014)	11-12
<i>Illinois v. Gates</i> , 462 U.S. 213 (1983)	3, 15, 17, 27
<i>In re Grand Jury Subpoenas</i> , 926 F.2d 847 (9th Cir. 1991)	24
<i>Kyllo v. United States</i> , 533 U.S. 27 (2001)	11
<i>Lyall v. City of Los Angeles</i> , 807 F.3d 1178 (9th Cir. 2015)	11
<i>Murray v. United States</i> , 487 U.S. 533 (1988)	14
<i>Riley v. California</i> , 134 S. Ct. 2473 (2014)	11
<i>United States v. Ackerman</i> , 831 F.3d 1292 (10th Cir. 2016)	9, 10, 12
<i>United States v. Artis</i> , 919 F.3d 1123 (9th Cir. 2019)	15
<i>United States v. Cameron</i> , 699 F.3d 621 (1st Cir. 2012)	13
<i>United States v. Chan</i> , 830 F. Supp. 531 (N.D. Cal. 1993)	10
<i>United States v. Cotterman</i> , 709 F.3d 952 (9th Cir. 2013)	10, 11
<i>United States v. Davis</i> , 332 F.3d 1163 (9th Cir. 2003)	14

1	<i>United States v. DeLeon,</i>	
	979 F.2d 761 (9th Cir. 1992)	
2	<i>United States v. Gourde,</i>	
3	440 F.3d 1065 (9th Cir. 2006)	15
4	<i>United States v. Hay,</i>	
	231 F.3d 630 (9th Cir. 2000)	18, 19
5	<i>United States v. Hawkins,</i>	
6	249 F.3d 867 (9th Cir. 2001)	13
7	<i>United States v. Jacobsen,</i>	
	466 U.S. 109 (1984)	11
8	<i>United States v. Johnson,</i>	
9	936 F.3d 1082 (9th Cir. 1991)	13
10	<i>United States v. Jones,</i>	
11	132 S. Ct. 945 (2012)	10
12	<i>United States v. Jones,</i>	
	565 U.S. 400 (2012)	11
13	<i>United States v. Keith,</i>	
14	980 F.Supp.2d 33 (D. Mass. 2013)	9, 12
15	<i>United States v. Kow,</i>	
	58 F.3d 423 (9th Cir. 1995)	26
16	<i>United States v. Lacy,</i>	
17	119 F.3d at 742 (9th Cir. 1997)	17, 18, 27
18	<i>United States v. Lien, 16-CR-393-RS,</i>	
19	2017 U.S. Dist. LEXIS 188903 (N.D. Cal. May 10, 2017)	13
20	<i>United States v. Lull,</i>	
	824 F.3d 109 (4th Cir. 2016)	28
21	<i>United States v. Lundin,</i>	
22	817 F.3d 1151 (9th Cir. 2016)	11
23	<i>United States v. Martinez-Garcia,</i>	
	397 F.3d 1205 (9th Cir. 2005)	15, 24
24	<i>United States v. Noufshar,</i>	
25	78 F.3d 1442 (9th Cir. 1996)	26
26	<i>United States v. Payton,</i>	
	573 F.3d 859 (9th Cir. 2009)	11
27	<i>U.S. v. Cofield, Case No. CR 19-00100-VC</i>	
28	DEF'S MOTION TO SUPPRESS	v

1	<i>United States v. Perkins,</i>	
	850 F.3d 1109 (9th Cir. 2017)	22
2	<i>United States v. Rabe,</i>	
3	848 F.2d 994 (9th Cir. 1988)	15, 17, 19, 27
4	<i>United States v. Raymonda,</i>	
	780 F.3d 105, 22 (2d Cir. 2015)	24
5	<i>United States v. Richardson,</i>	
6	607 F.3d 357 (4th Cir. 2010)	13
7	<i>United States v. Rosenschein, No. 16-CR-4571,</i>	
	2019 WL 2298810 (D.N.M. May 30, 2019).....	12
8	<i>United States v. Schesso,</i>	
9	730 F.3d 1040 (9th Cir. 2013)	<i>passim</i>
10	<i>United States v. Scott,</i>	
	705 F.3d 410 (9th Cir. 2012)	13
11	<i>United States v. Spilotro,</i>	
12	800 F.2d 959 (9th Cir. 1986)	26
13	<i>United States v. Stanert,</i>	
14	769 F.2d 1410 (9th Cir. 1985)	21, 22
15	<i>United States v. Stevenson,</i>	
	727 F.3d 826 (8th Cir. 2013)	13
16	<i>United States v. Stubbs,</i>	
17	873 F.2d 210 (9th Cir.1989)	27
18	<i>United States v. Vasey,</i>	
	834 F.2d 782 (9th Cir. 1987)	14
19	<i>United States v. Walther,</i>	
20	652 F.2d 788 (9th Cir. 1981)	12, 13
21	<i>United States v. Washington,</i>	
22	490 F.3d 765 (9th Cir. 2007)	14
23	<i>United States v. Weber,</i>	
	923 F.2d 1338 (9th Cir. 1990)	<i>passim</i>
24	<i>United States v. Wolfenbarger, 16-CR-00519-LHK,</i>	
25	2019 WL 6716357 (N.D. Cal. Dec. 10, 2019)	13
26	<i>VonderAhe v. Howland,</i>	
	508 F.2d 364 (9th Cir. 1974)	28, 29

1	<i>Wilson v. Russo</i> , 212 F.3d 781 (3d Cir. 2000)	22
2	<i>Wong Sun v. United States</i> , 371 U.S. 471 (1963)	14
3		
4	Federal Statutes	
5	18 U.S.C. § 2252	1, 2, 10
6	18 U.S.C. § 2258A	8, 9, 13
7	42 U.S.C. § 5773	9

INTRODUCTION

Ramon Cofield stands before this Court charged in a one-count indictment with possession of child pornography, in violation of 18 U.S.C. § 2252(a)(4)(B), (b)(2). He moves this Court to suppress all fruits of the unlawful searches of his private Tumblr, Google, and AT&T accounts, and his residence and the property found there.

FACTUAL BACKGROUND

As explained in greater detail below, on November 8, 2017, Tumblr created a CyberTipline Report, documenting the upload of a single image of alleged child pornography by Tumblr user chaz2076 on March 1, 2014. The Tumblr account was associated with the email rxxcofield@gmail.com. In accordance with its statutory obligations, Tumblr then sent the CyberTip to the National Center for Missing and Exploited Children (“NCMEC”). NCMEC conducted an investigation, and then submitted a report to law enforcement regarding the Tumblr account and the flagged image on this account.

After receiving NCMEC’s report, Sergeant Alicia Castillo of the San Francisco Police Department obtained several state search warrants: (1) on December 11, 2017, a warrant to search the chaz2076 Tumblr account (“Tumblr warrant”), (2) also on December 11, 2017, a warrant to search all of the Google products associated with the email rxxcofield@gmail.com (“Google warrant”), (3) on December 21, 2017, after obtaining the warrant return for the Google account information,² a search warrant for AT&T subscriber information for the telephone number associated with the rxxcofield@gmail.com account (“AT&T warrant”), and (4) on May 1, 2018, after obtaining the warrant returns for the three previous warrants, a warrant to search Mr. Cofield, his vehicles, and his San Francisco apartment (“Residence warrant”). According to Sgt. Castillo, the warrant searches of the Tumblr account, Google accounts, and search of Mr. Cofield and his apartment all returned images of child pornography and/or child erotica. At the time of his arrest, he was *Mirandized* and made incriminating statements.

On February 28, 2019, a grand jury returned an indictment charging Mr. Cofield with one count

² The warrant return from Google included a phone number associated with the account. SFPD ran a background check using that number, and connected it to Mr. Cofield.

1 of Possession of Child Pornography, in violation of 18 U.S.C. § 2252(a)(4)(B). Initially charged in state
 2 court, Mr. Cofield was re-arrested federally, arraigned, and released on stringent conditions, including
 3 electronic monitoring, on March 5, 2019. *See* ECF Nos. 5, 6. Since the beginning of the pandemic, he
 4 has primarily been sheltering-in-place due to his late-stage congestive heart failure and other health
 5 conditions that make him particularly vulnerable to Covid-19. Bischof Decl., ¶ 7. As a result of his
 6 long-term compliance on release and declining health, the electronic monitoring condition was removed.
 7 ECF No. 51.

8 **I. Tumblr's CyberTip and the NCMEC Report**

9 Tumblr is a microblogging service, on which users can post short images, video, music, text, or
 10 other media to their own personal Tumblr blog. Michel Decl., ¶ 4. On November 8, 2017, Tumblr
 11 created a NCMEC CyberTipline report which reflected that a Tumblr user had uploaded a single alleged
 12 child pornography image onto a Tumblr account on March 1, 2014. Bischof Decl., Ex. A (CyberTip No.
 13 25390444), USRC-5. Tumblr also reported account information, including a blog web url, numeric user
 14 name, and email and IP addresses associated with the Tumblr account. *Id.* at USRC-3. A Tumblr blog
 15 or any specific post may be public or private. Michel Decl. at ¶ 7. Tumblr's CyberTip provided no
 16 explanation of how it identified or located the suspected file inside the account. Bischof Decl., Ex. A.
 17 Tumblr's CyberTip also provided no explanation of *when* Tumblr discovered the image. *Id.* As part of
 18 its submission to NCMEC, Tumblr wrote "[w]e are attaching a representative sample of the blog's
 19 contents to this report" and also included posting information associated with 205 blog posts. *Id.* at
 20 USRC-3-7. The last login to the Tumblr account was on March 31, 2014. *Id.*

21 To this information, NCMEC added additional information from its own investigation
 22 concerning the IP address, which it identified as originating from AT&T U-verse in the San Francisco
 23 area. *Id.* at USRC-9. NCMEC forwarded the report to local law enforcement on November 21, 2017.
 24 *Id.* at USRC-12. It is not clear from the CyberTip report or the discovery provided in this case whether
 25 the specific image uploaded to the blog, rather than the hash value and corresponding image, was ever
 26 reviewed by a Tumblr employee before it was sent to NCMEC and SFPD. Although not explained in

the CyberTip report or set forth in the warrant application, PhotoDNA is a system developed by Microsoft and donated to NCMEC to assist law enforcement. *See* Microsoft PhotoDNA, at <https://www.microsoft.com/en-us/photodna> (last accessed November 30, 2020). Microsoft describes the system as follows: “PhotoDNA creates a unique digital signature (known as a ‘hash’) of an image which is then compared against signatures (hashes) of other photos to find copies of the same image.” *Id.* Images uploaded to Tumblr are matched against a shared database containing hashes of previously identified illegal images. *Id.*, *see also* Press Release, Internet Watch Foundation, *IWF Hash List announcement at Global Summit* (November 17, 2015), <https://www.iwf.org.uk/news/iwf-hash-list-announcement-at-global-summit>. As set forth in section IV, Tumblr’s parent company in 2017, Verizon Media, uses PhotoDNA to identify child exploitation material on all its platforms.

II. The Search Warrants

In December 2017, Sgt. Castillo applied for and obtained search warrants to Tumblr and Google. Bischof Decl., Exhibits B (Tumblr Warrant) and C (Google Warrant). The probable cause statements contained in the Google and Tumblr warrant applications are substantively identical.³

The probable cause statements in all four warrants contained the following paragraphs:

“Tumblr reported the following: On 11/08/17 at 21:12:00 UTC a Tumblr with the user name chaz2D76 with the IP Address of 162.238.124.187 utilizing the email of rxxcofield@gmail.com uploaded the filename: 78180748604.jpg to their Tumblr blog address of chaz2076.Tumblr.com In early part of 2014, beginning In February.”

Bischof Decl. Ex. B at USRC-232; Ex. C at USRC-177; Ex. D at USRC-111; Ex. E USRC-42. After affirming that she had reviewed the image and including a description, Sgt. Castillo further states:

“I conducted an online search for chaz2076.Tumblr.com and discovered several archived images of nude underage teenage males exposing their genitals that appeared to have been uploaded to Tumblr by chaz206 [sic] to another Tumblr user’s blog in 2014 .”

Id. In these two paragraphs, Sgt. Castillo recklessly misrepresented the following facts:

- she falsely stated that the child pornography image had been uploaded one month before she sought the Tumblr and Google search warrants, when in fact it was uploaded on March 1, 2014 (Ex. A at USRC-5), 45 months before she made the applications;
- she falsely stated that the tumblr user “utilize[ed]” the email address rxxcofield@gmail.com at

³ The Google probable cause statement adds a single paragraph which reads: “AFFIANT based on training and experience and the information supplied in the affidavit, is of the opinion that the items described are currently located at the above premises.” This adds nothing to meaningfully differentiate it from the Tumblr probable cause statement. Ex. C at USRC-177. This addition adds nothing to differentiate the probable cause statements because “[a] magistrate’s determination ‘cannot be a mere ratification of the bare conclusion of others.’ *Illinois v. Gates*, 462 U.S. at 230.

the time the image of child pornography was uploaded, when in fact a user only needs an email address to create an account, not post to it, and the CyberTip did not list the date the account was created (Michel Decl. at ¶ 6),

- she falsely stated that the Tumblr user had distributed images of “nude underage teenage males exposing their genitals” by uploading them to another user’s blog in 2014 when in fact Tumblr’s service does not offer the capability to upload photographs or other media to another user’s blog (Michel Decl. at ¶ 8).

In addition to the facts which were recklessly misrepresented, Sgt. Castillo also omitted numerous facts necessary to a probable cause determination:

- she failed to disclose that the Tumblr account had not been logged into since March 31, 2014 (Ex. A at USRC-3);
- she failed to disclose that a representative sample of other chaz2076 blog posts were reviewed and not flagged as child pornography (*Id.*);
- she failed to disclose that the date Tumblr discovered the image of child pornography was unknown (*Id.*);
- she failed to disclose that the image was identified with hashing technology or alternatively, that the method of discovery was unknown to her.

In addition to misrepresenting or omitting these facts, Sgt. Castillo also did not provide any necessary underlying information to suggest that child pornography might be stored electronically indefinitely, such as descriptions of the Tumblr or Google products she sought to search, the known characteristics of child pornography collectors, for instance, their habit of saving images and rarely disposing of them, or the ability of computer experts to retrieve deleted files. Indeed, she provided no averments whatsoever concerning the nature of electronically-stored contraband, or the habits of those who collect it. No protocol for sifting the requested data was proposed.

Based on this information, Sgt. Castillo sought from Tumblr:

Tumblr account associated with email address: rxxcofield@gmail.com and username chaz2076 for;

- All account information, subscriber names, user names, and other identities
- Email addresses, telephone numbers, and other contact information associated with Account
- Length of service of account
- List of followers as of 01/01/2014 and communication with individuals from 01/01/14 to present date
- IP connection log history of user access, and IP log information relating to account creation
- All images, links, videos uploaded and saved on account from 01/01/14 to present date.
- All blog posts from 01/01/14 to present date

Bischof Decl., Ex. B at USRC-228. And from Google, she sought:

- All account Information, email addresses, passwords, subscriber information, IP logs, methods of payment, communications with others between 01/01/2014- present date.
- Contents of the Inbox, sent box, all emails between 01/01/14- present date.

- Contents of Google drive and photos between 01/01/14 - present date.
 - Contents of Google+ photos account Including, but not limited to, photos stored, sent, and received between 01/01/14- present date.
 - Current contents of Google drive account and google photos.
- All associated with Google user accounts: rxxcofield@gmail.com

Ex. C, Google Warrant, at USRC-173. The Google probable cause statement does not include any information about how the Google email account is tied to any of the other Google accounts or information sought in the warrant, including Google Drive, Google Photos, emails, “communications,” etc. Nor does the Statement provide any information about how images are uploaded and/or stored in Google+, or how contraband could be in any of the other varied locations the warrant seeks to search.

III. Google Products

Google launched in 1995 as a search engine with two employees. Today it is a multinational corporation with 60,000 employees and hundreds of products. *See From the Garage to the Googleplex*, <https://www.google.com/intl/en/about/our-story/>. Among those products are Google+ (“Google Plus”), Google Photos, Google Drive, and Gmail.

Google+ is Google’s social networking service. *See* Marziah Karch, *The Beginner's Guide to Google+*, (October 7, 2016, updated March 27, 2020), <https://www.lifewire.com/what-is-google-definition-1616721>. Launched in 2011, it distinguished itself from other social networking sites (Facebook, MySpace, etc.) by offering organizational services like Circles (a way of separating online friends into subgroups), Hangouts (video chat and instant messaging), and Check-Ins (a way of telling friends where you are at any given time) that allowed users to connect to each other in unique ways. *Id.* Google+ also allows users to upload photos from their cell phones to their Google+ account. *Id.*

In 2015, Google launched “Google Photos”—a freestanding photo-storage site that allows users to upload, organize, and manipulate digital photographs. By May 2016, Google Photos had cached a breathtaking amount of information: 13.7 petabytes of data from over 200 million monthly users.⁴ *See* Anil Sabharwal, *Google Photos: One Year, 200 Million Users, and a Whole Lot of Selfies*, Official

⁴ To put that into perspective, 13 petabytes of music stored in MP3 format would take over 28,000 years to play. *See* Brian McKenna, *What Does a Petabyte Look Like?*, Computer Weekly.com (March 2013), <http://www.computerweekly.com/feature/What-does-a-petabyte-look-like>.
U.S. v. Cofield, Case No. CR 19-00100-VC

1 Google Photos Blog (May 27, 2016), [https://blog.google/products/photos/google-photos-one-year-200-](https://blog.google/products/photos/google-photos-one-year-200-million/)
2 million/.

3 Google Drive—launched in 2012, three years before Google Photos—is a multi-purpose cloud-
4 storage service. “Cloud storage” refers to a network of servers that store data and run software programs
5 remotely. *See* Jess Fee, *The Beginner’s Guide to the Cloud*, Mashable (Aug. 26, 2013),
6 <https://mashable.com/2013/08/26/what-is-the-cloud/>. Unlike Google Photos, Google Drive is built to
7 store all things digital, from receipts and office documents to home videos and high-school love letters.
8 As Google describes it, “[w]hether you’re working with a friend on a joint research project, planning a
9 wedding with your fiancé or tracking a budget with roommates, you can do it in Drive.” Sundar Pichai,
10 *Introducing Google Drive... Yes, Really*, Google’s Official Blog (April 24, 2012),
11 <https://googleblog.blogspot.no/2012/04/introducing-google-drive-yes-really.html>.

12 Because Google Drive allows users to “[s]tore [their] files securely and access them from any
13 device,” *Drive Help*, <https://support.google.com/drive/answer/2424384?>, users store the same
14 information on Google Drive that they would store on a hard drive in their home: “tax returns and other
15 financial information, health records, books, music and virtually any other imaginable content.” Lon A.
16 Berk, *After Jones, the Deluge: The Fourth Amendment's Treatment of Information, Big Data and the*
17 *Cloud*, 14 J. High Tech. L. 1 (2014).

18 Finally, Gmail is Google’s wildly popular email product. Launched (in non-beta form) in 2009,
19 at the time Sgt. Castillo authored the Google search warrant, Gmail had over one billion users. *See*
20 Ross Miller, *Gmail Now Has 1 Billion Monthly Active Users*, The Verge (Feb. 1, 2016),
21 <http://www.theverge.com/2016/2/1/10889492/gmail-1-billion-google-alphabet>.

22 Google+, Google Photos, Google Drive, and Gmail have two things in common: first, they are
23 all Google products; second, because they are all Google products, they all use the account holder’s
24 Gmail address as the local account username. (So, for instance, if John Smith had a Google Drive and
25 a Google+ account, his username for both accounts would be his Gmail address.) Other than that, the
26 four products are wholly separate, with no more in common than, for instance, Facebook (a Google+

competitor), Shutterfly (a Google Photos competitor), Dropbox (a Google Drive competitor), and Hotmail (a Gmail competitor). A post written in Google+ is not automatically relayed to Gmail; an email sent from Gmail is not automatically saved in Google Drive; a photo stored in Google Drive does not automatically appear in Google Photos; and a photo album in Google Photos is not automatically available on Google+.

IV. Tumblr and Law Enforcement

Tumblr was purchased by Yahoo! in 2013. *See* Chris Isidore, *Yahoo buys Tumblr, promises to not 'screw it up'* CNN (May 20, 2013, 4:24 PM), <https://money.cnn.com/2013/05/20/technology/yahoo-buys-tumblr/index.html>. In 2017, Yahoo! and by extension, Tumblr, were acquired by Verizon Media. *See* Vindu Goel, *Verizon Completes \$4.48 Billion Purchase of Yahoo, Ending an Era*, New York Times, (June 13, 2017), <https://www.nytimes.com/2017/06/13/technology/yahoo-verizon-marissa-mayer.html>. Verizon Media uses “[c]utting-edge technology, including PhotoDNA, that scans images and videos uploaded to our platforms against databases of known child sexual abuse material” in order to find and remove child exploitation material and identify the responsible parties for law enforcement. *See What is Verizon doing to combat online child exploitation?*, <https://www.verizon.com/about/our-company/company-policies/digital-safety> (last accessed November 29, 2020). They employ “[i]n-house investigators who develop and transmit to NCMEC attribution information about offenders who traffic in child sexual abuse material on our platforms” and a “dedicated team that reviews material flagged by our scanning technology, proactively searches for material in flagged accounts that may have missed by automated scanning, and takes action on user reports of child sexual abuse material.” *Id.*

Yahoo! and Verizon have long partnered with NCMEC; Verizon Media is a corporate sponsor at the “Protector” level, meaning it makes “significant [annual] contributions at the highest level” and “[i]n addition to its financial contributions, Verizon supports NCMEC’s mission by donating online advertising across its owned and operated digital media properties.” *See* Press Release, “*Verizon Joins With the National Center for Missing and Exploited Children to Fight Online Child Pornography*,” (March 28, 2008), <https://www.verizon.com/about/news/press-releases/verizon-joins-national-center->

1 missing-and-exploited-children-fight-online-child-pornography; *see also* NCMEC – Our Corporate
2 Partners, *available at* <https://www.missingkids.org/supportus/our-corporate-partners>. Yahoo! was a
3 founding member of NCMEC’s public-private Technology Coalition as well as its Financial Coalition
4 Against Child Pornography. Press Release, “Statement from Microsoft on Establishment of Technology
5 Coalition within National Center for Missing and Exploited Children,” June 27, 2006,
6 [https://news.microsoft.com/2006/06/27/statement-from-microsoft-on-establishment-of-technology-](https://news.microsoft.com/2006/06/27/statement-from-microsoft-on-establishment-of-technology-coalition-within-national-center-for-missing-and-exploited-children/)
7 [coalition-within-national-center-for-missing-and-exploited-children/](https://news.microsoft.com/2006/06/27/statement-from-microsoft-on-establishment-of-technology-coalition-within-national-center-for-missing-and-exploited-children/) *see also* Government Technology,
8 “Financial and Internet Industries To Combat Internet Child Pornography,” March 28, 2006, *available at*
9 <https://www.govtech.com/security/Financial-and-Internet-Industries-To-Combat.html>. According to
10 NCMEC: “The Technology Coalition [was] funded within NCMEC to develop and deploy technology
11 solutions that disrupt the ability of predators to use the Internet to exploit children or traffic in child
12 pornography.” Press Release, “Google Joins Industry-Wide Movement to Combat Child Pornography,”
13 <https://www.icmec.org/press/google-joins-industry-wide-movement-to-combat-child-pornography/>. Its
14 purpose is “to enhance knowledge sharing among industry participants, *improve law enforcement tools*,
15 and research perpetrators’ technologies in order to enhance industry efforts and build solutions.” *Id.*
16 (emphasis added).

17 Within the United States, Tumblr is also statutorily obligated to report any child pornography it
18 discovers to NCMEC. 18 U.S.C. § 2258A(a). Its report may include “the identity of any individual who
19 appears to have violated a Federal law” involving child pornography, “the electronic mail address,
20 Internet Protocol address, uniform resource locator, or any other identifying information, including self-
21 reported identifying information” for that individual, his or her geographic location, and any image of
22 suspected child pornography relating to the incident underlying the report. 18 U.S.C. § 2258A(b). If
23 Tumblr fails to make a report, it faces a \$150,000 fine for a first offense, and a \$300,000 fine for each
24 offense thereafter. 18 U.S.C. § 2258A(e).

25 \\
26 \\
27

V. NCMEC

Although the Ninth Circuit has never addressed the issue, NCMEC has been deemed by other courts to be both a government actor and a government entity. *United States v. Ackerman*, 831 F.3d 1292, 1296 (10th Cir. 2016), *reh'g denied* (Oct. 4, 2016); *see also, United States v. Keith*, 980 F.Supp.2d 33, 40-43 (D. Mass. 2013). NCMEC's two authorizing statutes—18 U.S.C. § 2258A and 42 U.S.C. § 5773(b)—mandate its collaboration with federal, state, and local agencies “in over a dozen ways.”

Ackerman, 831 F.3d at 1296. NCMEC is, for instance, statutorily obligated

to operate the official national clearinghouse for information about missing and exploited children, to help law enforcement locate and recover missing and exploited children, to “provide forensic technical assistance . . . to law enforcement” to help identify victims of child exploitation, to track and identify patterns of attempted child abductions for law enforcement purposes, to “provide training . . . to law enforcement agencies in identifying and locating non-compliant sex offenders,” and . . . to operate the CyberTipline as a means of combating Internet child sexual exploitation.

Id. (citing 42 U.S.C. § 5773(b)). Significantly, NCMEC is also funded heavily by the federal government. In the period relevant to this case, 2016-18, the U.S. Department of Justice funded NCMEC to the tune of \$28.3 million annually (constituting the largest share of funding distributed by the Department's Missing and Exploited Children program). *See* Congressional Research Service, The Missing and Exploited Children's (MEC) Program: Background and Policies (July 29, 2019), pp. 7 (Table 1), *at* <https://fas.org/sgp/crs/misc/RL34050.pdf>.

NCMEC's rights and responsibilities regarding child pornography are specific. Service Providers such as Tumblr are required to report any known image of child pornography to NCMEC, rather than federal or local law enforcement. 18 U.S.C. §§ 2258A(a)(1) & (g)(2)(B)(i). When NCMEC confirms that it has received a report from an ISP, it “must treat that confirmation as a request to preserve evidence issued by the government itself,” *Ackerman*, 831 F.3d at 1297, is permitted to “receive [any attached child pornography] knowingly and to review its contents intentionally,” *id.*, and must subsequently “transmit [that] report[], including relevant images and information, to the appropriate international, Federal, State or local law enforcement agency for investigation,” 42 U.S.C. § 5773. These

are rights and responsibilities that “Congress has extended to NCMEC alone . . . specifically to assist or support law enforcement agencies in administration of criminal justice functions.” *Ackerman*, 831 F.3d at 1297 (citation and quotations marks omitted). By contrast, and unlike NCMEC, private parties would ordinarily risk prosecution by knowingly receiving and reviewing child pornography. *See* 18 U.S.C. § 2252A(a)(2) (receipt); *id.* § 2252A(a)(5)(B) (possession). Notably, however, NCMEC is authorized to provide technical information from the CyberTip reports NCMEC generates—*i.e.*, “hash values or other unique identifiers associated with a specific visual depiction, including an Internet location and any other elements provided in a CyberTipline report,” except child pornography images—to service providers such as Tumblr to enable “the provider to stop the online sexual exploitation of children.” 18 U.S.C. § 2252C(a)(1) & (a)(2). No other private parties, other than service providers, are authorized to receive such information from NCMEC to assist in enforcement activity. *Id.*

ARGUMENT

I. The Government Bears the Burden of Proving That the Warrantless Searches Fell Within an Exception to the Fourth Amendment’s Warrant Requirement

“The Fourth Amendment provides in relevant part that ‘[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated.’” *United States v. Jones*, 132 S. Ct. 945, 949 (2012) (quoting U.S. Const. amend. IV). The digital information stored on Mr. Cofield’s Tumblr and Google accounts implicates the Fourth Amendment’s specific guarantee of an individual’s right to be secure in his “papers.” This follows from the fact that information stored on electronic servers, like the electronic servers supporting Google and Tumblr’s products, includes “the same kind of highly sensitive data one would have in ‘papers’ at home.” *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013); *see also, e.g., United States v. Chan*, 830 F. Supp. 531, 534 (N.D. Cal. 1993) (“The expectation of privacy in an electronic repository for personal data is . . . analogous to that in a personal address book or other repository for such information.”).

Electronic services such as Gmail, Google+, Google Drive, and Tumblr are, like laptops, iPads, cell phones, and other instruments of modern information storage, “simultaneously offices and personal diaries,” private, digital compartments that “contain the most intimate details of our lives.” *Cotterman*, 709 F.3d at 965; *see also Riley v. California*, 134 S. Ct. 2473, 2491 (2014) (Fourth Amendment protects cell phones in part because of their “immense storage capacity,” resulting in part from their access to information stored “in the cloud”); *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009) (“Searches of computers . . . often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers.”). Because these electronic services contain the same intensely intimate information as their physical counterparts, they trigger the same constitutional protections. *See Kyllo v. United States*, 533 U.S. 27, 34 (2001) (emphasizing that evolving technology cannot be allowed to “erode the privacy guaranteed by the Fourth Amendment”).

A. NCMEC and Tumblr, Acting as Government Agents, or as a Government Entity and its Agent, Respectively, Conducted Unconstitutional Searches of Mr. Cofield’s Tumblr Account

A “search” occurs, for Fourth Amendment purposes, in two circumstances. It occurs, first, when the government or an entity acting as a government agent infringes “an expectation of privacy that society is prepared to consider reasonable.” *United States v. Jacobsen*, 466 U.S. 109, 113 (1984). It occurs, second, when the government or its agent intrudes or trespasses upon a constitutionally protected area—“persons, houses, papers, [or] effects”—to obtain information. *United States v. Jones*, 565 U.S. 400, 405 (2012); *see also Lyall v. City of Los Angeles*, 807 F.3d 1178, 1185 (9th Cir. 2015) (“[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.” (citation and quotation marks omitted) (emphasis in original)); *United States v. Lundin*, 817 F.3d 1151, 1158 (9th Cir. 2016) (crediting *Jones*’ property-right conception of Fourth Amendment analysis).

Under either theory, Mr. Cofield’s Tumblr account was subjected to at least three warrantless searches: (1) Tumblr’s original search of the files in his Tumblr account; (2) NCMEC’s subsequent search of the image forwarded by Tumblr to NCMEC; and (3) Sgt. Castillo’s final search of the same

1 image. While the conduct of a private citizen or organization ordinarily would not be attributable to the
2 state, both Tumblr and NCMEC were acting as government agents when they searched the contents of
3 Mr. Cofield's Tumblr account. *See George v. Edholm*, 752 F.3d 1206, 1215 (9th Cir. 2014) ("A private
4 party's search may be attributed to the state when 'the private party acted as an instrument or agent of
5 the Government' in conducting the search." (quoting *Skinner v. Ry. Labor Execs.' Ass'n*, 489 U.S. 602,
6 614 (1989)); *Keith*, 980 F.Supp.2d at 40-43 (holding that NCMEC was acting as a government agent
7 under similar circumstances). NCMEC, moreover, also qualifies as a government entity. *See*
8 *Ackerman*, 831 F.3d at 1295-1301 (holding that NCMEC is a government entity).

9 In cases where a search was allegedly conducted by a non-governmental actor, the question of
10 whether the Fourth Amendment applies to that search requires consideration of "(1) the government's
11 knowledge and acquiescence, and (2) the intent of the party performing the search." *United States v.*
12 *Walther*, 652 F.2d 788, 192 (9th Cir. 1981). The Ninth Circuit applied this test in *Walther*, and
13 concluded that the employee who performed the search had acted as an agent of the government. *Id.* at
14 793. In that case, the employee who performed the challenged search worked for an airline named
15 Western Airlines. *Id.* at 789. While so employed, he opened a case and found white powder, and
16 contacted the DEA. *Id.* The case was then packed. *Id.* This employee had opened packages in the past
17 and made prior reports to the DEA as a paid informant. *Id.* at 790. The Ninth Circuit considered
18 whether that individual employee was acting as a government agent in the context of that search, and
19 concluded that he was. *Id.* at 793.

20 Applying the same two-factor test in *United States v. Ackerman*, 831 F.3d 1292, 1296-97 (10th
21 Cir. 2016), the Tenth Circuit, in an opinion authored by then-Judge Neil Gorsuch, concluded that
22 NCMEC functioned as a government entity for purposes of the Fourth Amendment, rendering its actions
23 subject to the Fourth Amendment's warrant requirement. *See Ackerman*, 831 F.3d at 1296; *see also*
24 *United States v. Rosenschein*, No. 16-CR-4571, 2019 WL 2298810 (D.N.M. May 30, 2019) (finding
25 NCMEC is a member of the prosecution team sufficient to trigger discovery obligations under Rule 16).
26 Here, there is no question that the government, at least through the government entity NCMEC, knew of

1 and acquiesced in Tumblr and NCMEC's joint conduct. The government not only collaborates with
 2 both organizations to ferret out child pornography, but it also statutorily mandates their participation.
 3 *See* 18 U.S.C. § 2258A. Here, the record shows that Tumblr and NCMEC work together through the
 4 Technology Coalition and other NCMEC subgroups to improve law enforcement tools, and build
 5 solutions through collective knowledge of perpetrators' technologies. And, just as was the case for the
 6 informant in *Walther*, Tumblr and NCMEC have a long track record of assisting the government—and
 7 NCMEC is even primarily financed by the Department of Justice. *Walther*, 652 F.2d at 790. Verizon
 8 Media employs special investigators whose job description mandates that they “develop and transmit to
 9 NCMEC attribution information about offenders.” In this case, both Tumblr and NCMEC assumed a law
 10 enforcement role by proactively investigating the Mr. Cofield's account. Tumblr actively searched his
 11 files, and reported his IP address, while NCMEC took the affirmative steps of investigating the IP
 12 address and forwarding information concerning the location and owner of the IP address to SFPD.

13 Mr. Cofield acknowledges, as he must, that the weight of precedent in this District and across
 14 the country does not support the view that electronic service providers have acted as government agents
 15 in similar circumstances.⁵ Nevertheless, the Ninth Circuit has yet to weigh in on this emerging area of
 16 the law. Mr. Cofield therefore respectfully requests a ruling to secure his rights.

17 B. The Government Cannot Establish that Any Exception to the Fourth Amendment's
 18 Warrant Requirement Applies

19 It is well established that any warrantless search is *per se* unreasonable, subject only to a few
 20 well-delineated exceptions. *United States v. Scott*, 705 F.3d 410, 416 (9th Cir. 2012); *United States v.*
 21 *Hawkins*, 249 F.3d 867, 872 (9th Cir. 2001). For that reason, “[t]he burden of proving that a warrantless
 22 search or seizure falls within an exception to the warrant requirement is on the government.” *Scott*, 705
 23 F.3d at 416 (citing *Hawkins*, 249 F.3d at 872); *see also United States v. Johnson*, 936 F.3d 1082, 1084
 24 (9th Cir. 1991) (“The government bears the burden of justifying a warrantless search.”). The

25 ⁵ *United States v. Stevenson*, 727 F.3d 826, 830 (8th Cir. 2013); *United States v. Cameron*, 699 F.3d 621 (1st Cir. 2012);
 26 *United States v. Richardson*, 607 F.3d 357, 367 (4th Cir. 2010); *United States v. Wolfenbarger*, 16-CR-00519-LHK, 2019
 27 WL 6716357 (N.D. Cal. Dec. 10, 2019); *United States v. Viramontes*, 16-CR-508-EMC, ECF No. 62 (N. D. Cal. Nov. 14,
 28 *U.S. v. Cofield*, Case No. CR 19-00100-VC

government must prove that any exception applies by a preponderance of the evidence. *United States v. Vasey*, 834 F.2d 782, 785 (9th Cir. 1987).

Mr. Cofield invites the government to demonstrate that each of the presumptively unreasonable searches in this case was lawful. He submits, however, that the government will be unable to meet its burden and therefore that all evidence obtained as a result of these Fourth Amendment violations must be suppressed as “fruit of the poisonous tree.” See *Wong Sun v. United States*, 371 U.S. 471, 488 (1963); *United States v. Washington*, 490 F.3d 765, 775 (9th Cir. 2007) (quoting *Wong Sun*, 371 U.S. at 488) (“[E]vidence obtained subsequent to a violation of the Fourth Amendment is tainted by the illegality and is inadmissible . . . unless the evidence obtained was ‘purged of the primary taint.’”); *United States v. Davis*, 332 F.3d 1163, 1170-71 (9th Cir. 2003) (“[T]he standard articulated in *Wong Sun* remains the relevant test.”).

II. SFPD’s State Search Warrants Were Invalid

The state search warrants obtained by Sgt. Castillo to search Mr. Cofield’s Tumblr account and various Google accounts also violated the Fourth Amendment for several reasons. First, as an initial matter, the statement of probable cause filed in support of the warrant relied on information obtained by Sgt. Castillo from Tumblr’s and NCMEC’s unlawful warrantless searches. Second, and even more clearly fatal, the probable cause statements were riddled with material misrepresentations and omissions of fact, without which probable cause would have been lacking. Finally, the Statement was insufficient to establish probable cause that contraband likely would be found in each of the many areas the Tumblr and Google warrants sought to search. Both individually and collectively, these facts require suppression of the fruits of the search of Mr. Cofield’s Tumblr and Google accounts.

A. The Probable Cause Statements Relied Primarily Upon the Fruits of Tumblr, NCMEC, and SFPD’s Presumptively Unconstitutional Searches

As an initial matter, all fruits of the warrant search of Mr. Cofield’s Google and Tumblr accounts must be suppressed because the warrant itself was tainted fruit from the initial warrantless searches by Tumblr and NCMEC, which, as discussed above, violated the Fourth Amendment. See, e.g., *Murray v. United States*, 487 U.S. 533, 536-42 (1988) (exclusionary rule applies to warrant if

U.S. v. Cofield, Case No. CR 19-00100-VC
DEF’S MOTION TO SUPPRESS

information from prior illegal search was material to magistrate’s decision to issue it). Here, all of the information provided in support of the Tumblr and Google search warrant applications was provided by Tumblr and NCMEC to Sgt. Castillo; without such, there was no information whatsoever to justify a finding of probable cause. The AT&T and Residence warrant applications were also based on information by Tumblr and NCMEC and supplemented by fruits of that information obtained in the Tumblr and Google search warrant returns. Finally, “the good-faith exception may not be invoked when ‘the search warrant was issued in part on the basis of evidence obtained from an illegal search.’” *United States v. Artis*, 919 F.3d 1123, 1133 (9th Cir. 2019) (quoting *United States v. Wanless*, 882 F.2d 1459, 1466-67 (9th Cir. 1989)).

B. Sergeant Castillo Made False Statements and Omitted Critical Information In Her Warrant Applications

Under *Franks v. Delaware*, 438 U.S. 154 (1978), a defendant is entitled to an evidentiary hearing if he makes a “substantial preliminary showing” (1) that law enforcement officers made a false statement or omission “knowingly and intentionally, or with reckless disregard for the truth,” and (2) that statement or omission was “necessary to the finding of probable cause.” *United States v. Martinez-Garcia*, 397 F.3d 1205, 1214 (9th Cir. 2005) (quoting *Franks*, 438 U.S. at 155-56). A probable cause determination depends upon the “totality of the circumstances,” *Illinois v. Gates*, 462 U.S. 213, 230-31 (1983), and “applies with equal force to cases involving child pornography on a computer,” *United States v. Gourde*, 440 F.3d 1065, 1069 (9th Cir. 2006). Before a search warrant issues, the government must “establish by sworn evidence presented to a magistrate that probable cause exists to believe that an offense has been committed and that items related to that offense . . . will be found on the premises sought to be searched at the time the warrant is issued.” *United States v. Rabe*, 848 F.2d 994, 997 (9th Cir. 1988); *see also Gates*, 462 U.S. at 238. Probable cause in this context means a “fair probability that contraband or evidence is located in a particular place.” *Gates*, 462 U.S. at 231. That probability is based on a probable cause statement, which must present enough information for a magistrate independently to determine probable cause. The magistrate’s determination “cannot be a mere ratification of the bare conclusion of others.” *Gates*, 462 U.S. at 230. If the officer acted recklessly or

intentionally, then “the search warrant must be voided and the fruits of the search excluded.” *Franks*, 438 U.S. at 156.

Here, Sgt. Castillo’s bare bones, three-page probable cause statements in the Tumblr and Google search warrants have a half page of information upon which a magistrate could base a probable cause determination, and the entire half page is infected by material false statements and omissions. Bischof Decl., Exs. B at USRC-232; C at USRC-177.

Sgt. Castillo’s false statements and omissions fell into three major categories: 1) those that obscured the staleness of the evidence, 2) those that fabricated probable cause to believe the suspect was engaged in a broader scope of criminal activity such as distribution and thus created a nexus between the conduct alleged in the warrant and the broad universe of items sought in the Tumblr and Google accounts, and 3) those that falsely fashioned an inference that the suspect was engaged in a continuing pattern of criminal activity using the Tumblr or Google accounts, such that it would be likely that more child pornography would be found in those accounts.

i. Sgt. Castillo Falsely Stated that the Image of Child Pornography Had Been Uploaded on November 8, 2017, and the User “Utilized” the Gmail Address During the Upload

After outlining her training and experience and giving a brief description of the services Tumblr provides, Sgt. Castillo wrote:

“Tumblr reported the following:

On 11/08/17 at 21:12:00 UTC a Tumblr with the user name **chaz2076** with the IP Address of **162.238.124.187** utilizing the email of rxxcofield@gmail.com uploaded the filename: **78180748604.jpg** to their Tumblr blog address of **chaz2076.tumblr.com** in early part of 2014, beginning in February.”

Ex. B at USRC-232; Ex. C at USRC-177, emphasis in the original.

Conversely, the NCMEC CyberTipline Report generated by Tumblr and NCMEC indicates that the image in question was uploaded on March 1, 2014. Ex. A at USRC-5. It clearly states that November 8, 2017, was the time that the NCMEC “report was created in Tumblr’s system” not when the image was uploaded or discovered. *Id.* at USRC-3. Moreover, a Tumblr user only needs to access an email address to sign up for the service, not when logging in or uploading posts to their Tumblr blog. Michel Decl., ¶

1 6. That means that there was no necessary connection between the Gmail account and the Tumblr
2 account after the creation of the Tumblr account. The creation date *was not disclosed* in the CyberTip.
3 These misstatements functioned to mislead the issuing magistrate into believing that the warrant was not
4 stale.

5 Before a search warrant issues, the government must “establish by sworn evidence presented to a
6 magistrate that probable cause exists to believe that an offense has been committed and that items
7 related to that offense . . . will be found on the premises sought to be searched at the time the warrant is
8 issued.” *United States v. Rabe*, 848 F.2d 994, 997 (9th Cir. 1988); *see also Illinois v. Gates*, 462 U.S.
9 213, 238 (1983). In *United States v. Lacy*, the Ninth Circuit explained the test for staleness in the context
10 of an investigation of electronically-stored child pornography: “‘We evaluate staleness in light of the
11 particular facts of the case and the nature of the criminal activity and property sought.’” 119 F.3d at 745
12 (quoting *United States v. Pitts*, 6 F.3d 1366, 1369 (9th Cir. 1993). “The information offered in support
13 of the application for a search warrant is not stale if ‘there is sufficient basis to believe, based on a
14 continuing pattern or other good reasons, that the items to be seized are still on the premises.’” *Id.* at
15 745-46 (quoting *United States v. Gann*, 732 F.2d 714, 722 (9th Cir. 1984)). However, the Ninth Circuit
16 specifically warned that, “[w]e are unwilling to assume that collectors of child pornography keep their
17 materials indefinitely,” *id.* at 746 (emphasis added), and then went on to require that the supporting
18 declaration must provide specific, “good reasons” to believe that the contraband would likely be found
19 in the place to be searched even after a delay. *Id.* As this Court is no doubt aware, it has now long been
20 standard practice for investigators to include such averments to justify delays in the collection of
21 electronic evidence. *See, e.g., United States v. Schesso*, 730 F.3d 1040, 1047 (9th Cir. 2013) (relying on
22 affidavit swearing that “individuals who possess child pornography ‘rarely, if ever, dispose of sexually
23 explicit images of children’ because these images are treated as ‘prized possessions’”), *see also United*
24 *States v. Greathouse*, 297 F. Supp. 2d 1264, 1270-73 (D. Or. 2003) (13-month-long delay too long and
25 information was stale given the showing of probable cause presented in the affiant's October 2001
26 search warrant application was based entirely on a single report from September 2000 that a user named

1 “cyotee” was offering Internet access to files containing child pornography, there was no evidence of
2 any ongoing criminal activity involving the defendant or the use of the name “cyotee” during the
3 yearlong time period leading to the issuance of the warrant and given that “no explanation or
4 justification for such a significant delay was ever offered”).

5 Similarly, here, the probable cause statements are worded to convey the false impression that the
6 child pornography was uploaded and Gmail address used only one month prior, when in fact it had been
7 nearly four years. This misstatement is especially egregious because the probable cause statements set
8 forth only a single upload and do not include the date the child pornography was discovered or the
9 account was created. Without knowing *when* Tumblr learned of the child pornography, the reviewing
10 court simply could not make any determination concerning the likelihood that it would still be found in
11 the Tumblr account. To the extent Sgt. Castillo may attempt to rely on her statement that she received
12 the CyberTip on November 30, 2017, that is immaterial and does not assist to establish probable cause
13 because there are no facts recited to link the timing of her receipt of the CyberTip report to the time of
14 Tumblr’s original discovery. CyberTip reports may languish for months or years before an investigator
15 receives or follows up on them. Thus, the time of her receipt of the CyberTip report does not
16 meaningfully inform the reviewing court of when Tumblr originally discovered the child pornography.
17 Moreover, without knowing *when* the Tumblr account was created, the reviewing court could not know
18 if the suspect used the Gmail account close in time to the upload of child pornography, creating a nexus
19 between the two.

20 The probable cause statements are similarly void of any basic facts, like those set forth in
21 *Schesso*, concerning the nature of electronically-stored child pornography and the habits of those who
22 collect it. Without a discovery date, or that basic background information, the warrant is plainly invalid.
23 The Ninth Circuit’s case law requires “good reasons” to justify a delayed electronic search that may
24 include, at a minimum: “a continuing pattern” of criminal activity, *see Lacy*, 119 F.3d at 745-46
25 (quoting *Gann*, 732 F.2d 714); information explaining why child pornography collectors choose the
26 particular form of electronic media at issue to permanently store contraband, *Hay*, 231 F.3d at 636;

assurances that “even if [the defendant] had deleted the files, they could nevertheless be retrieved by a computer expert,” *Hay*, 231 F.3d at 636; incriminating information about the profile of the particular individual associated with the account, *see United States v. Weber*, 923 F.2d 1338, 1344-45 (9th Cir. 1990) (discussing *United States v. Rabe*, 848 F.2d 994, 995 (9th Cir. 1988)); or information about “the known characteristics of child pornography collectors,” including their habit of saving images and rarely disposing of them, *Schesso*, 730 F.3d at 1047. The complete absence of these very basic contextual averments is in stark contrast to those detailed declarations that have been upheld under similar circumstances by the Ninth Circuit. *See, e.g., United States v. Hay*, 231 F.3d 630, 635-36 (9th Cir. 2000).

In *Hay*, the court expounded on the importance of these expert averments, which although seemingly just boilerplate, provide an essential basis for a finding of probable cause in child pornography investigations:

[T]he boilerplate in [the detective’s] affidavit provides context for Evans’s transfer of 19 images to Hay’s Internet address, and forms the basis upon which the magistrate judge could plausibly conclude that those files were still on the premises. It sets forth relevant background information about how child pornography is traded and distributed over the Internet: through use of chat rooms to establish contacts, followed by transmission or trading of images. It points out that the computer’s ability to store images in digital form makes it an ideal repository for child pornography. The affidavit also explains that the computer has become one of the preferred methods of distribution of child pornographic materials and opines, based upon Galante’s experience and that of colleagues, that searches and seizures of evidence from computers requires agents to seize all parts of a computer system to be processed later by a qualified computer expert. *See United States v. Gil*, 58 F.3d 1414, 1418 (9th Cir. 1995) (“[W]hen interpreting seemingly innocent conduct, the court issuing the warrant is entitled to rely on the training and experience of police officers.”). In sum, the affidavit (including “boilerplate” based on the agents’ experience), provides a substantial basis for the probable cause determination.

Hay, 231 F.3d at 636.

By contrast, the statement in this case contained *none of this standard supporting information*. The only other conduct described appears to be legal conduct that is equally remote.⁶ The only other information Sgt. Castillo provided was a generic description of the Tumblr product, untethered to any

⁶ Sgt. Castillo offers no basis for a magistrate to determine that the images of nude males were either “child” -the descriptor teenage by definition means pubescent - or “pornography” – defined in this context as either a sex act or a lascivious display. The pictures themselves were not attached to the search warrant applications.

1 explanation as to why it would likely be a permanent repository of child pornography. She does not
 2 even address the uses of the Google products, such as whether they offer the capacity to store images,
 3 what amounts of data, and for how long. Without the implication that the upload was recent, there is no
 4 basis upon which a magistrate could conclude that the conduct was a “continuing pattern” or that there
 5 were other “good reasons” to justify a delayed electronic search of Mr. Cofield’s Tumblr account or
 6 Google accounts.

7 **ii. Sgt. Castillo Falsely Stated that Mr. Cofield Uploaded Images to Another User’s Blog**

8 After falsely stating that an image of child pornography was uploaded to the chaz2076 blog in
 9 2017, and describing her impressions of that image, Sgt. Castillo concludes the substantive portion of
 10 the probable cause statements by claiming:

11 “I conducted an online search for chaz2076,tumblr.com and discovered several archived
 12 images of nude underage teenage males exposing their genitals that **appeared to have
 been uploaded to Tumblr by chaz206 [sic] to another Tumblr user's blog in 2014.**”
 Ex. B at USRC-232; Ex. C at USRC-177, emphasis added.

13 However, Tumblr’s service does not offer the capability to upload photographs or other media to
 14 another user’s blog, so it would have been impossible for Mr. Cofield to share material with another
 15 user in this way. Michel Decl., ¶ 8. Based on this statement, Sgt. Castillo sought a broad universe of
 16 items, including, among other things, all “communications with others” in all Google services, the
 17 contents of Mr. Cofield’s Google Drive, and the entire “[c]ontent of [Cofield’s] Inbox, [and] sent box,”
 18 as well as “all emails between 01/01/14- present date [12/2017].” Ex. C at USRC-173. Her false
 19 statement served to convince the magistrate court that a nexus existed between the observed conduct
 20 and “communications with others” in the Tumblr and Google accounts.

21 Without conveying the false impression that Mr. Cofield had *distributed* sexual material involving
 22 minors, the probable cause statement provides a magistrate no reason to believe that Mr. Cofield, after
 23 uploading a single image of child pornography, would have had “communications with others” about
 24 child pornography or child exploitation or related subjects. *See e.g. Weber*, 923 F.2d at 1341 (even
 25 general descriptions of characteristics of pornography collectors or pedophiles were insufficient to
 26 establish probable cause to search for, among other things, “correspondence” where conduct was receipt

of one order of child pornography and possible order of apparent child pornography two years prior). The false statement is particularly significant because, again, the probable cause statement is void of even generalized information about how individuals who are accused of child pornography offenses may or may not use the particular electronic services Sgt. Castillo sought to search, or any “characteristics of child pornographers” that might suggest that Mr. Cofield would have kept contraband in other locations or shared it or communicated about it with others. To seek a search warrant for a Gmail account on the basis of contraband in a Tumblr account is like seeking a search warrant for a Hotmail account because an image was uploaded to Facebook. There is simply nothing connecting the two services, and no evidence that email was ever used to upload, transport, or view any images. Without falsely claiming that Mr. Cofield had distributed sexual content, Sgt. Castillo could not establish probable cause to search for communications with others on Tumblr and Google platforms, or to search the Google platforms for additional child pornography images.

iii. Sgt. Castillo Recklessly Omitted the Facts that the Tumblr Account Had Not Been Logged Into for Over Three Years, that a Representative Sample of the Blog Was Reviewed and No Further Child Pornography Was Found, Child Pornography Image Was Identified Using Hashing Technology, and that the Date Tumblr Discovered the Child Pornography Was Unknown

Sgt. Castillo omitted several facts from the probable cause statements that indicated that the upload of child pornography was likely a single, isolated event, and that more child pornography was unlikely to be found in the Tumblr or Google accounts. *Franks* applies not only to falsehoods, but also to “deliberate or reckless *omissions* of fact which tend to mislead.” *United States v. Stanert*, 762 F.2d 775, 781, *amended* 769 F.2d 1410 (9th Cir. 1985) (emphasis added).

The use of deliberately falsified information is not the only way by which police officers can mislead a magistrate when making a probable cause determination. *By reporting less than the total story, an affiant can manipulate the inferences a magistrate will draw.* To allow a magistrate to be misled in such a manner could denude the probable cause requirement of all real meaning.

Id. (emphasis added). In the case of such intentional or reckless omissions, the court must review the warrant application “with the omitted information included” and determine whether the application would still establish probable cause. *United States v. DeLeon*, 979 F.2d 761, 764 (9th Cir. 1992). If not,

the warrant is invalid and any fruits obtained via the warrant must be suppressed. Where a *Franks* claim is based upon material omissions from a warrant affidavit, a law enforcement officer acts with reckless disregard for the truth when he “withholds a fact in his ken that ‘any reasonable person would have known that this was the kind of thing the judge would wish to know.’” *Wilson v. Russo*, 212 F.3d 781, 788 (3d Cir. 2000) (quoting *United States v. Jacobs*, 986 F.2d 1231, 1235 (8th Cir. 1993)); *see also id.* at 787 (acknowledging that “reckless disregard for the truth means different things when dealing with omissions and assertions”); *Chism v. Washington*, 661 F.3d 380, 388 (9th Cir. 2011) (“The most commonsense evidence that the officer acted with at least a reckless disregard for the truth is that the omissions and false statements contained in the affidavit were all facts that were within [the officer’s] personal knowledge.”). These intentional or, at best, reckless omissions undermine the warrants’ validity. *See United States v. Perkins*, 850 F.3d 1109, 1118 (9th Cir. 2017) (citing *United States v. Stanert*, 762 F.2d 775, 781 (9th Cir. 1985) (“We have recognized that an affiant can mislead a magistrate ‘[b]y reporting less than the total story, [thereby] ... manipul[at]ing the inferences a magistrate will draw.”). To be clear, the issue “is not that the statements in the affidavit were false, but rather that [the officer], by not disclosing that he had drawn an inference but instead presenting the inference as an empirical fact, usurped the inference-drawing function of the magistrate in determining probable cause.” *State v. Castagnola*, 46 N.E.3d 638, 650 (Ohio 2015); *see also Perkins*, 850 F.3d at 1118 (“By providing an incomplete and misleading recitation of the facts and withholding the images, [the agent] effectively usurped the magistrate’s duty to conduct an independent evaluation of probable cause.” (citation omitted)).

Here, Sgt. Castillo’s probable cause statements excluded four critical points: 1) she failed to disclose that the Tumblr account had not been logged into since March 31, 2014; 2) she failed to disclose that a representative sample of other chaz2076 blog posts were reviewed and not flagged as child pornography; 3) she failed to disclose that the date Tumblr discovered the image of child pornography was unknown; and 4) she failed to disclose that the image was identified with hashing technology or alternatively, that the method of discovery was unknown to her. Each of these omissions

1 undercut the magistrate's ability to believe that additional child pornography would be found in Mr.
2 Cofield's Tumblr account or in Mr. Cofield's associated Google accounts.

3 The CyberTipline Report indicates that the last login to Tumblr account chaz2076 occurred on
4 March 31, 2014. Bischof Decl., Ex. A at USRC-3. By omitting that the account had not been logged into
5 since 2014, Sgt. Castillo manipulated the magistrate's impression (especially when combined with the
6 misstatement that the illegal image was uploaded in 2017) that the user who uploaded the child
7 pornography continued to access and post to the blog. This manipulation was compounded by her failure
8 to state that a representative sample of other chaz2076 blog posts were reviewed and not flagged as child
9 pornography. As part of its submission to NCMEC, Tumblr wrote "[w]e are attaching a representative
10 sample of the blog's contents to this report." Bischof Decl., Ex. A at USRC-3. Based on their inclusion
11 of IP address information associated with certain postings, it appears they may have included up to 205
12 blog posts. *Id.* at USRC-USRC5-7. Regardless of the number, they were termed "representative" and no
13 other child pornography was identified. These omissions, separately and collectively, cemented the
14 impression produced by her other false statements: that the upload of child pornography was not stale,
15 and that more contraband was likely to be found in the Tumblr and Google accounts because the
16 conduct amounted to a continuing pattern.

17 On top of the omissions discussed above, Sgt. Castillo also intentionally or recklessly omitted
18 key information concerning how Tumblr identified the child pornography and the associated account,
19 and the fact that the date of discovery was unknown. In particular, Sgt. Castillo concealed that the
20 image had been identified by the PhotoDNA algorithm, neglected to explain how the hashing
21 technology works, and failed to state whether anyone at Tumblr contemporaneously viewed the image
22 before forwarding it to NCMEC and ultimately law enforcement. Because the child pornography image
23 was almost certainly identified by its hash value, and Tumblr searches every upload, it would have been
24 reasonable for the magistrate to infer any other known child pornography would likely have been
25 uncovered as well, especially over the three year period the blog lay dormant. Combined with the fact
26 that only a single image was found, these omissions further undermine any conclusion that contraband

1 would likely be found in the Tumblr account or associated Gmail account, since there was no indication
2 of a larger, and possibly persistent, collection, let alone clearly criminal activity. See e.g. *Weber*, 923
3 F.2d 1338 (absent proof that defendant collected child pornography, controlled delivery of a single order
4 of child pornography did not establish probable cause to search for other illegal images in his home);
5 *United States v. Raymonda*, 780 F.3d 105, 22 117 (2d Cir. 2015) (evidence that defendant briefly viewed
6 thumbnail of child pornography absent any other circumstances suggesting that the suspect had accessed
7 the images deliberately or had a continuing interest in child pornography failed to support probable
8 cause that defendant hoarded such images).

9 Separately, each of Sgt. Castillo's reckless misrepresentations and omissions is fatal to probable
10 cause. Together, they present an indisputably false picture of a suspect who has recently uploaded child
11 pornography to a limitless blog and distributed multiple sexual images of teenage males with another
12 Tumblr, rather than presenting an accurate picture of a remote-in-time single upload of child
13 pornography to a long-abandoned account, discovered by an automated service likely to identify any
14 other such images, but which found none. Sgt. Castillo's misrepresentations and omissions establish a
15 *Franks* violation. See *Martinez-Garcia*, 397 F.3d at 1214 (holding that a *Franks* violation exists where
16 there is reckless disregard for the truth and the misrepresentation or omission was necessary to the
17 probable cause finding). There can be no question that Sgt. Castillo was at least reckless in stating,
18 without *any* evidence, that the upload occurred in 2017, that the user chaz2076 intentionally distributed
19 images of nude teens to another Tumblr user. Without these false statements – especially in light of Sgt.
20 Castillo's omissions of exonerating evidence- there was no evidence whatsoever to show that the
21 evidence was not stale, there was any nexus between the conduct and Mr. Cofield's "communications"
22 or any of his Google accounts, or that more child pornography would be found on the chaz2076 Tumblr
23 or rxxcofield Google accounts. This critical portion of the warrant application therefore lacked probable
24 cause, and the evidence returned should be excluded. See *Franks*, 438 U.S. at 156.

C. The State Search Warrant Failed to Meet the Fourth Amendment's Specificity Requirement

In order for a search to be reasonable under the Fourth Amendment, the warrant must be specific. *In re Grand Jury Subpoenas*, 926 F.2d 847, 856 (9th Cir. 1991). Specificity has two requirements: breadth (that probable cause limit the warrant's scope) and particularity (that the warrant clearly state what is sought). *Id.*; see also *United States v. Weber*, 923 F.2d. 1338, 1342 (9th Cir. 1991). Under the breadth requirement, generic classifications in a warrant "are acceptable only when a more precise description is not possible." *Id.* (quoting *United States v. Bright*, 630 F.2d 804, 812 (5th Cir.1980)).

The search warrants issued for the contents of Mr. Cofield's Tumblr and Google accounts were overbroad in multiple respects. First, it required Google to turn over all "communications," and "emails" in Mr. Cofield's account "between 01/01/14- present date [12/2017]," a 47-month period. Bischof Decl., Ex. C at USRC-173. Similarly, Tumblr was required to produce all "communication with individuals from 01/01/14 to present date [12/2017]." Bischof Decl., Ex. B at USRC-228-229. As explained in the Background section, *supra*, Google's product are not connected to one another. Other than the fact that Mr. Cofield (like all Google account holders) uses his Google email address as the username for his Google+ account, the two products have nothing to do with one another. Even if they were somehow connected, there is no evidence that Mr. Cofield shared child pornography, whether by email or otherwise. Because there was no evidence that Mr. Cofield sent or received illegal images via email, chat or other "communications", no probable cause supported a search of his email or Tumblr chat accounts.

Second, the warrant required Google to turn over the entire "[c]ontents of Google drive and photos between 01/01/14- present date [12/2017]." Bischof Decl., Ex. C at USRC-173. Here, again, the warrant conflates Google's products. Google Drive and Google Photos are separate products that provide distinct services. (See the description of these products, *supra*.) While both products technically allow users to store photos, there is little reason to store photos in Google Drive, which offers none of the photo editing and networking tools Google Photos does and, unlike Google Photos, charges for storage space. See Derek Walter, *Choosing Between Google Photos or Google Drive for Image*

Backups, Green Bot (Jan. 18, 2017), <http://www.greenbot.com/article/3156927/android/choosing->
U.S. v. Cofield, Case No. CR 19-00100-VC
 DEF'S MOTION TO SUPPRESS

1 between-google-photos-or-
2 google-drive-for-image-backups.html. Additionally, the warrant application did not even attempt to
3 show a link between these products or otherwise attempt to explain why Sergeant Castillo believed
4 probable cause existed to search them when the CyberTip indicated only that a Gmail email was used to
5 sign up for the Tumblr account that housed the single child pornography image.

6 Even if there were some link between Google Photos and Google Drive, no evidence suggested
7 that Mr. Cofield stored photos anywhere but in his Tumblr account. And even if it did, that would not
8 amount to probable cause to search his *entire* Drive account, which, again, may have held anything from
9 “tax returns and other financial information, health records, books, [and] music [to] virtually any other
10 imaginable content.” *Berk, supra*. Because the evidence in the warrant application did not even attempt
11 to support an inference that Mr. Cofield had uploaded child pornography to his Google Drive account,
12 there was no probable cause to search it.

13 Finally, the warrant lacked particularity, for it did not “set out objective standards by which
14 executing officers c[ould] differentiate items subject to seizure from those which are not.” *United States*
15 *v. Noufshar*, 78 F.3d 1442, 1447 (9th Cir. 1996). While the warrant identified the Tumblr and Google
16 products the government sought to search—Gmail, Google+, Google Photos, and Google Drive—it
17 “contained no limitations on which documents within each category could be seized or suggest[] how
18 they related to specific criminal activity.” *United States v. Kow*, 58 F.3d 423, 427 (9th Cir. 1995).
19 Instead, the warrant “authorize[d] wholesale seizures of entire categories of items [that are] not
20 generally evidence of criminal activity”—from shopping receipts to tax returns—“and provide[d] no
21 guidelines to distinguish items used lawfully from those the government had probable cause to seize.”
22 *United States v. Spilotro*, 800 F.2d 959, 964 (9th Cir. 1986). Even the date limitations, which purport to
23 impose broad boundaries, in fact do not. Do they limit the search to files that had been accessed between
24 the dates listed? Do they include files saved prior to those dates but never accessed (essentially including
25 every item ever saved on the Drive)? Do they include files “deleted” yet still in the “trash” folder? The
26 warrant does not say.

Because it sets no limits on the type of content Google had to return, “the warrant is indistinguishable from the general warrants repeatedly held by [the Ninth Circuit] court to be unconstitutional.” *Id*; see, e.g., *United States v. Rabe*, 848 F.2d 994, 998 (9th Cir. 1988) (warrant overbroad where it “authorize[d] seizure of [defendant’s] financial and telephone records without providing any guidelines to aid the officer in determining what may or may not be seized”); *United States v. Stubbs*, 873 F.2d 210, 211 (9th Cir.1989) (warrant invalid “because of the complete lack of any standard by which an executing officer could determine what to seize”).

For the forgoing reasons, the state search warrant failed to satisfy the Fourth Amendment’s specificity requirement. The resulting search violated the Fourth Amendment, and its fruits should be suppressed.

D. The Tumblr and Google Search Warrants Lacked Probable Cause

Even setting aside the rampant false statements and omissions in the probable cause statements, they were woefully inadequate. Before a search warrant issues, the government must “establish by sworn evidence presented to a magistrate that probable cause exists to believe that an offense has been committed and that items related to that offense . . . will be found on the premises sought to be searched at the time the warrant is issued.” *Rabe*, 848 F.2d at 997 (9th Cir. 1988); see also *Gates*, 462 U.S. at 238, see also Section II B, for general statement of the law.

The Ninth Circuit has made abundantly clear that “law enforcement and judicial officers must be especially cognizant of privacy risks when drafting and executing search warrants for electronic evidence.” *United States v. Schesso*, 730 F.3d 1040, 1042 (9th Cir. 2013). *Schesso* found probable cause for the search where the search warrant application: (1) described a video the defendant had downloaded and the agents had seen; (2) confirmed that the defendant had uploaded and distributed the video through a peer-to-peer network designed for sharing; (3) explained the operation of that network and described the storage capacity of the electronic evidence to be searched; (4) explained how the internet is generally used to distribute child pornography; and (5) identified the known characteristics of child pornography collectors. *Id.* at 1043. In *Lacy*, the Ninth Circuit similarly relied on an affidavit that

1 specifically outlined the characteristics of child pornography collectors to retain their collections for
2 long periods of time. *Id.* at 745-46 (“Based on her training and experience as a Customs agent, the
3 affiant explained that collectors and distributors of child pornography value their sexually explicit
4 materials highly, ‘rarely if ever’ dispose of such material, and store it ‘for long periods’ in a secure
5 place, typically in their homes.”).

6 No such information was included in this case. At best, Sgt. Castillo’s affidavit provided
7 probable cause to search for the single image of child pornography uploaded to the chaz2076 Tumblr
8 blog. Even here, however, Sgt. Castillo’s application fell short. First, as explained above, it was not
9 disclosed how Tumblr identified, reviewed, and reported information to NCMEC and law enforcement,
10 leaving one to guess at the method’s reliability or recency. *See Lull*, 824 F.3d at 116–17 (affiant’s
11 omission of facts about an informant’s credibility “usurp[ed] the magistrate’s role” in determining
12 probable cause).

13 Second, the warrant’s nominal limitations on the Google+ account search—“[c]ontents of
14 Google+ photos account including, but not limited to, photos stored, sent, and received between
15 01/01/14- present date [12/2017]” Ex. C at USRC-173—provides no limitation at all. If the warrant
16 includes, *but is not limited to*, the photographs in the provided date range, then it includes any photo Mr.
17 Cofield *has ever stored* in his Google+ account. *See, e.g., VonderAhe v. Howland*, 508 F.2d 364, 369
18 (9th Cir. 1974). But the fact that the probable cause statements asserts that a single image of child
19 pornography was uploaded to an account associated with the rxxcofield Gmail address in November
20 2017 does not provide probable cause to search every photo Mr. Cofield has ever stored in his Google
21 accounts. That, of course, is one reason why Sgt. Castillo provided a date range in the first place. But the
22 date range does not actually limit the search.

23 Third, even if the search were properly limited, Sgt. Castillo’s warrant affidavit provides no reason
24 to think that more images would be located in Mr. Cofield’s Tumblr or Google accounts. “[P]robable
25 cause to believe that *some* incriminating evidence will be present at a particular place does not
26 necessarily mean there is probable cause to believe that there will be more of the same.” *Weber*, 923

F.2d. at 1344 (citing *VonderAhe*, 508 F.2d at 370 (emphasis in original)). Sgt. Castillo should have provided, at a minimum, known characteristics of pornography collectors, as the affiant did in *Schesso*, and explained why Tumblr’s hashing technology would not have identified those other images, if they existed. The defense has been unable to locate any child pornography case in the Ninth Circuit that comes close to presenting such a drastic lapse by law enforcement, let alone one where the validity of the search was upheld. Instead, as noted above, a review of the case law shows that it has been law enforcement’s standard practice for many years, and in every case reported, to provide the information that is plainly missing here when applying for a warrant targeting electronically-stored child pornography. Without that information, there was no way for the magistrate credibly to suspect that more contraband would be found in Mr. Cofield’s Tumblr or Google accounts.

In short, based on the information and circumstances contained in the four corners of the warrant, there was insufficient probable cause even to search Mr. Cofield’s Tumblr or Google. The evidence obtained from the search—even the search of the Tumblr account—must be suppressed.

III. The Warrants Issued to Search AT&T and Mr. Cofield and His Residence Were Invalid

Not only did the third and fourth warrants SFPD sought rely upon the same defective information as the state warrant, as outlined above, they also included detailed descriptions of the evidence obtained from the invalid Tumblr and Google warrant searches and are therefore textbook “fruit of the poisonous tree” that must be suppressed. Bischof Decl., Exs. D; E.

CONCLUSION

For all these reasons, Mr. Cofield respectfully requests that the Court grant his motion to suppress.

Dated: November 30, 2020

Respectfully submitted,

/s

GABRIELA BISCHOF
Attorney for Defendant